

Stopping Cybercrime

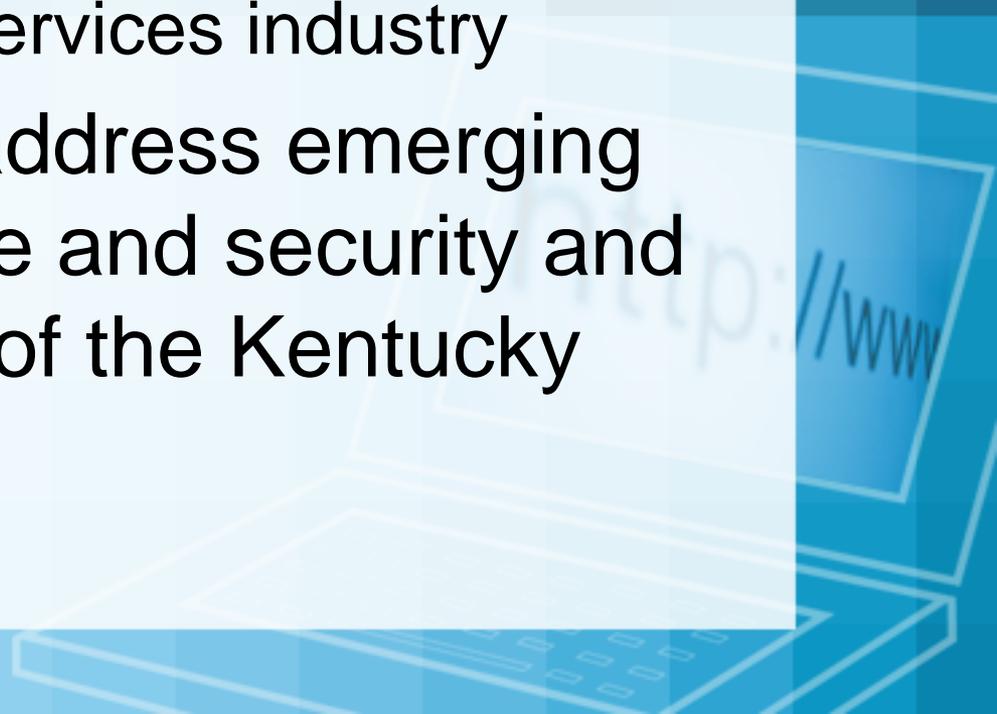
Tips for Consumers

A presentation by the
**Financial Cybercrime
Task Force of Kentucky**
KY Dept. of Financial Institutions



Task Force Role

- The Financial Cybercrime Task Force of Kentucky:
 - DFI internal work group
 - Offers guidance and warnings for the Kentucky financial services industry
- Goal: Identify and address emerging threats in cybercrime and security and protect the integrity of the Kentucky financial system



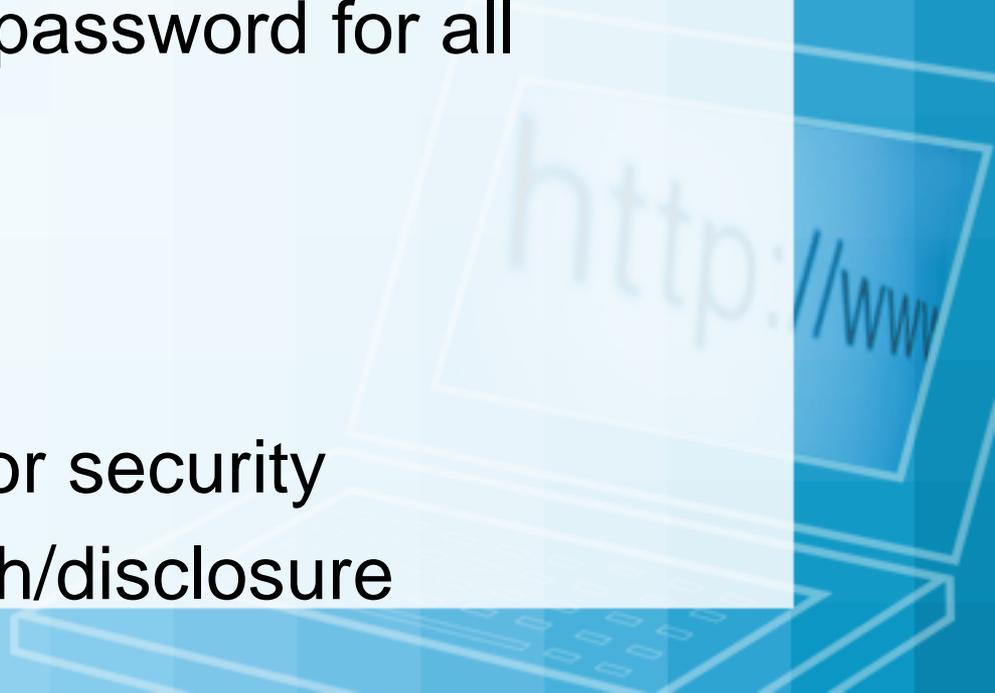
Hardware and Software

- Virus/malware protection
- Update software and install patches
 - *All* software – not just virus protection
- Password protect home networks
 - Never auto-fill or “remember” passwords



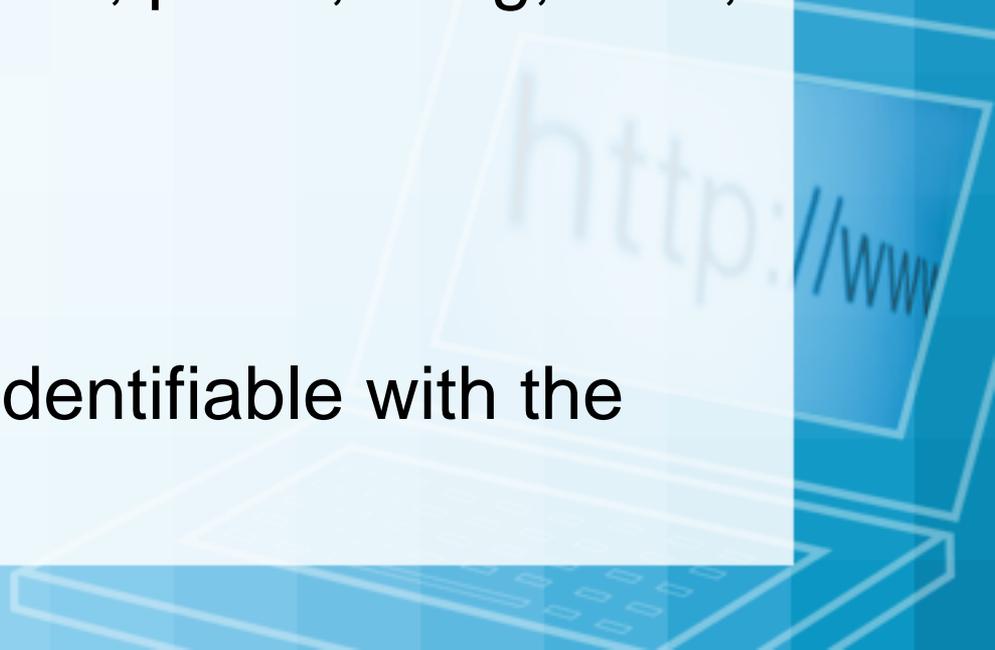
Passwords

- Choose 2-factor authentication
- Make it unique
 - Don't use manufacturer default or temporary passwords
 - Don't use the same password for all accounts
- Keep it confidential
- Change passwords
 - Every so often just for security
 - Immediately if breach/disclosure



POOR Passwords and PINs

- Passwords should NOT:
 - Repeat letters or numbers or use sequences
 - Use whole words or common phrases
 - Name a specific person, place, thing, date, etc.
- PINs should NOT:
 - Be a number easily identifiable with the user



STRONG Passwords

- **DO Create Passwords that:**
 - Are 8 or more characters
 - Contain uppercase and lowercase letters
 - Contain a number
 - Contain a special character
 - Are unpredictable

Example of a Strong Password:

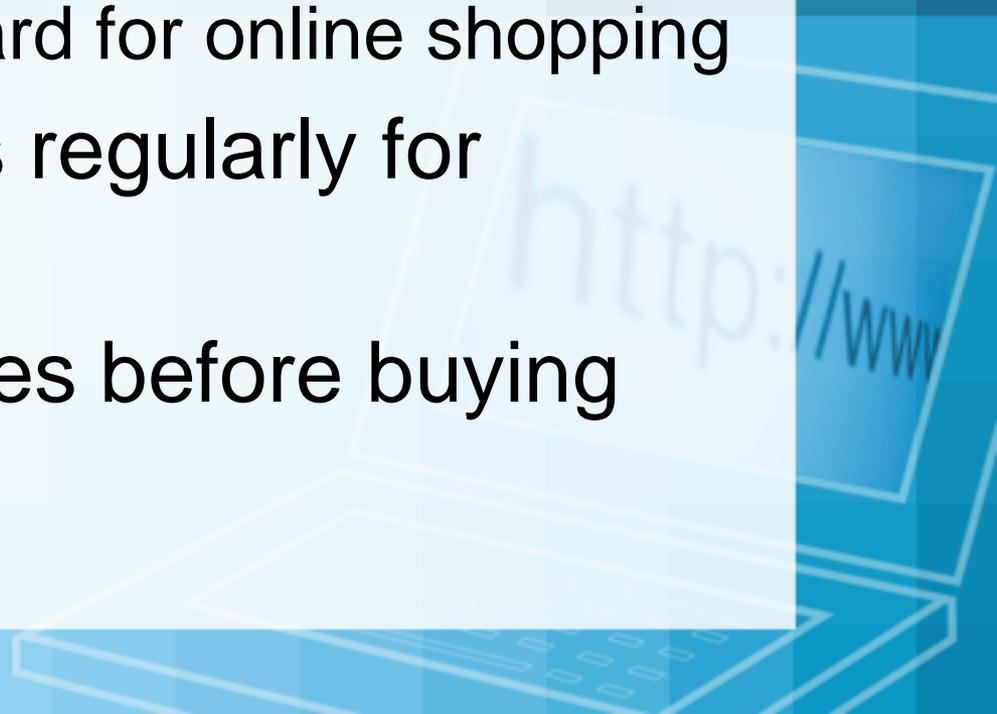
Prot3ctYfc!

= Protect Yourself From Cybercrime!



Banking and Shopping

- Only give info over encrypted websites
 - Your bank will never ask for your personal information by email or phone
 - Look for “https” in the web address
 - Use a designated card for online shopping
- Review transactions regularly for unusual activity
- Check out businesses before buying



Clicking, sharing, saving ...

- Never give out personal information over telephone, fax, email, social media
- Beware of emails and attachments
 - If unsolicited, don't open it
 - If from a friend, still be cautious
- Back up your files
- Be wary online



Other Tips

- GPS – “Home”
- Cell phone – Labels/identifiers



Questions or Reports

- Contact the Task Force at dfi.reporting@ky.gov
 - To report financial cybercrime or potential attacks
 - If you have questions or suggestions
- <http://kfi.ky.gov/industry/Pages/cybercrime.aspx>
- <http://www.onguardonline.gov/topics/secure-your-computer>